RISK MANAGEMENT DIVISION

CONTINGENCY PLAN

Revised: **June 5, 2002**

TABLE OF CONTENTS

1. OVERVIEW

1.1 PURPOSE

A disaster is defined as the occurrence of any event that causes a significant disruption in Risk Management Division capabilities. The central theme of this Plan is to minimize the effect a disaster will have upon the Division's on-going operations. The Plan responds to the most severe disaster, the kind that requires moving off site to a backup facility. Occurrences of a less severe nature are controlled at the appropriate level as a part of the total Plan.

This Disaster Contingency Plan for the Risk Management Division will be used to respond to any failure that impacts the Division's ability to operate. It includes:

1.2 OBJECTIVES

The role of this Plan in these objectives is to document the pre-agreed decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the Division and its services.

This Disaster Contingency Plan's objectives are to:

Protect the Division's resources and employees;

1. Safeguard the Division's vital records of which the Division has become the custodian;
2. Guarantee the continued availability of essential Risk Management Division services;
3. Permit immediate, accurate and measured response to emergency situations;
4. Minimize the number of time-critical decisions that Risk Management personnel will need to make when a failure occurs;
5. Minimize the impact of a disaster-related failure on Risk Management's mission;
6. Minimize a failure's effect on day to day operations (i.e. ensure smooth, effective transition from normal to backup operations); and
7. Expedite restoration of normal operations and failed facilities or equipment.

1.3 ASSUMPTIONS

The Plan assumes that:

1. A catastrophic event has severely crippled the operation forcing it to reestablish full operations at a fully equipped backup facility.
2. All applications will eventually be processed at the backup location, even those not classified as critical.
3. Failure of disaster remediation activities is assumed in the contingency development.
4. The contingency must be operable for the duration of the interruption.
5. If a failure occurs, the necessary personnel (or their backups) will be both available and capable of completing their responsibilities as described in this Plan.
6. If a backup site or facility has been designated, it will be accessible to staff.
7. As part of the initial start-up at the backup site, "mission critical" functions will be run first.
8. Access to up to date version of all Risk Management Server Net (RMNSVRNT) file data (H:, P:, R:, U:, and W: Drives). This information can be downloaded from ITD mainframe.
9. Although this Plan follows the assumption of a catastrophic disaster, the Plan can be quickly altered to handle a less severe emergency as determined by management.

2. IMMEDIATE RESPONSE

As soon as an emergency situation happens, the on-site personnel should contact the appropriate emergency authorities and then take the necessary steps to minimize property damage and injury to people in the vicinity.

2.1 Problem Identification:

This Contingency Plan will be activated if a failure occurs in a business process that impedes the normal flow of work for more than **two** days.

2.2 Notification:

Crisis Management Team -

Team Leader:

Jo Zschomler – Office 328-6510 – Cell 391-3485 – Home Phone Number
Home E-Mail Address
Home Address

Derek Watkins – Office 328-6513 – Cell 391-3037 – Home Phone Number
Home E-Mail Address
Home Address

Risk Management Staff:

Vicki Lewis – Office 328-6511 – Cell 391-3486 – Home Phone Number
Home E-Mail Address
Home Address

Terry Milas – Office 328-6512 – Cell 391-3486 – Home Phone Number
Home E-Mail Address
Home Address

Renae Schumacher – Office – 328-6514 – Home Phone Number
Home E-Mail Address
Home Address

All staff will report their status to team leaders in the event of a catastrophic event.

In the event notification of status of operations from a Team Leader has not been made and efforts to make contact with Risk Management Division Staff have failed, access the Risk Management Division Home Page or the North Dakota Web Site at www.discovernd.com for communication and instructions if possible.

2.3 Activation Criteria

Based on contingency triggers, the Crisis Management Team will:

a) activate contingency plan, or
b) cancel the alert and resolve the emergency through usual business practices.

2.4 Problem Report:

Provide details on the failure, to include IT, Embedded Systems, Process, Infrastructure, Suppliers, or Customers, to:

Contact List:

1) OMB Director

2) Fire and Tornado Fund if there is a loss:
   a) Make temporary repairs so further damage does not occur.
   b) Notify Fire and Tornado Fund (328-9600) immediately.
   c) Complete a Notice of Loss Form (SFN 9576) by referencing inventory listing from P:\Equipment Files\Inventory.xls) and forward to Fire and Tornado Fund.

3) ITD:
   a) Work on restoring files from backup.
   b) Restore programs (Windows, RiskKey, PhotoSuite, Flextraining, etc.)

4) Temporary forward mailing address to the alternate site:
   a) Post Office
   b) Presort
   c) Capitol Mail Room

5) Contact State and Local Telephone Service to transfer:
   a) Telephone calls to the alternate site.
   b) FAX messages to OMB FAX number or alternate site.

2.5 Media Relations

Staff will not speak to the media.

If a statement becomes unavoidable then this statement may be made, "At Risk Management we don't speculate about any interruption, we are awaiting the findings of the State's Emergency Response Team."

3. DETAILED CONTINGENCY PLAN

3.1 Exposures and Contingency Triggers per Critical Function

Exposure

Critical functions/processes and their vulnerability to failures.

1. Loss of documentation of events and claims.
2. Loss of documentation used to facilitate settlement of valid claims.
3. Loss of documentation used to provide basis to deny a claim.
4. Loss of documentation used to validate a claim (timely filing).
5. Inaccurate Reserves.

6. Loss of history used to determine contributions to the Risk Management Fund.

Impact

1. Corrupt or lost files.
2. Irrational data.
3. Loss of documentation of financial viability of the Risk Management Fund.
4. Wrongfully denying a valid claim.
5. Wrongfully paying an invalid claim.
6. Inaccurate reports.
7. Inaccurate assessment of required contributions.

Trigger

1. Irretrievable System shutdown.
2. Irretrievable System hang-up.
3. Inability to access data.
4. Interruption of internal and external communications.

3.2 Component/Process

1. Locate at alternate business site (as determined by the Emergency Relocation Team (701-328-6514)), or Risk Management personnel's residence, depending on space availability.

2. Data entry will be reestablished at the alternate site through the laptops and the call-in modem in a reasonably short time (depending on ITD workload).

3. The current telephone and FAX numbers must be forwarded/transferred to the alternate site or OMB.

4. Special office equipment critical to the operation are copier and FAX functions which can be accessed at OMB at the Capitol or other State Offices in the City of Bismarck.

5. Use credit card to purchase office supplies such as paper, ink cartridges, etc.

6. Maintain cost documents of personal expenses for office supplies and equipment.

7. While in a stand by mode we will continue to receive incidents and claims. They will be entered into the RMIS when it becomes operational.

8. Revise Notice of Claim correspondence to claimants stating "due to electronic failures there may be a delay in responding to claims."

9. During work stoppage manual recording and filing systems will be maintained.

10. During the catch up mode backlogged data will be entered from hard copy to ensure all manually recorded information is included.

11. Normalization is when the system is restored and backlog is cleared.

4. RETURN TO NORMAL OPERATIONS

Checklist:

1. Meet with staff about interim move.
2. Coordinate interim requirements.
3. Coordinate relocation schedules with others.
4. Inform external contacts of external location/process.
5. Inform vendors/partners of external location/process.
6. Verify operational readiness.
7. Execute move.

5. APPENDICES

5.1 Inventory considerations:

Hardware:

1. A copy of the inventory of all computer hardware and communication equipment including serial numbers and software program licenses, is listed on P:\Equipment Files\Inventory.xls).

2. The communication network will quickly connect with the Dial-in Network for email. If the Risk Management Server Net (RMNSRVNT) (H:, P:, R:, U:, and W: Drives) is damaged, ITD should download the saved information and reconfigure access to the files.

3. Printers are maintained at the alternate sites.

Software:

   1. Application software, license, and technical manuals would be replaced by the vendors pursuant contract. A documented license numbers list is located at P: \ Equipment Files \ Risk Management Software Inventory List.

2. Contact ITD to execute on another system during an emergency.

3. RiskKey disc will be maintained off site at the Team Leader's residence.

5.2 Vital Records Inventory

Files:

1. The backup facility is the ITD Mainframe which is backed up every night 5 generations (last 5 updates) can be recovered, can be retrieved in about 1 day after notification by calling ITD.
2. A copy of the Risk Management Division Contingency Plan is maintained on the backed up files on the P: drive.
3. For restart procedures for all production systems, contact ITD Help Desk (328-4470).